P801456/WO/1

DaimlerChrysler AG


## Abstract

The invention relates to a simplified symmetrical, cryptographic method. The basis of this method is an authentication code. This authentication code is calculated in a secured area, referred to as a trust center, by concatenating the application program, referred to as the flashware, with a secret data string and calculating a hash value from the concatenated application program. This hash value is calculated here by means of the application program and by means of the secret data string. This hash value is the authentication code for the application program to be checked. The authentication code is checked in the microprocessor system or in the control unit in which the application program is to be used. For this purpose, a second, identical, secret data string is stored in the microprocessor system or the control unit. Firstly, the unencrypted application program and the authentication code are transmitted into the microprocessor system or into the control unit. The unencrypted application program is then concatenated with the second, identical, secret data string in the microprocessor system or in the control unit. A hash value is calculated by this concatenated application program in the microprocessor system or in the control unit. If the calculated hash value and the transmitted authentication code correspond, the transmitted application program or the transmitted flashware is considered to be authentic and is allowed to be stored in the flash memory and applied in the control unit or in the microprocessor system. In a development of the invention, the application program is concatenated with the secret data string at both ends both at the start of the program and at the end of the program. The hash value is then calculated by means of the application program which is concatenated at both ends. In order to

check the authentication code which is formed in this way, in the microprocessor system or in the control unit the application program which is transmitted in unencrypted form is also concatenated at both ends with the second, secret data string stored in the control unit, and a hash value is formed in the control unit or in the microprocessor system by means of the application program which is concatenated at both ends. If the hash value calculated in the control unit or in the microprocessor system corresponds to the transmitted authentication code, the transmitted application program is considered to be authentic. The concatenation at both ends has the advantage of improved protection against unacceptable manipulations of the application software.